**LISTING OF CLAIMS**

1.    (Previously Presented) A method comprising:

       receiving at a device driver a network packet having a corresponding security association (SA);

       determining if the packet is an ingress packet or an egress packet;

       determining for the packet a key value corresponding to the SA;

       if the packet is an ingress packet, hashing the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hashing the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;

       retrieving from the entry an index to a location of the SA in memory; and

       retrieving the SA from memory based on the index.


2.    (Previously Presented) The method of claim 1 wherein receiving the network packet comprises the device driver being passed an egress packet from an electronic system operating system.


3.    (Previously Presented) The method of claim 1 wherein receiving the network packet comprises the device driver being passed an ingress packet from a network interface device.


4.    (Original) The method of claim 1 wherein the key value is a handle created for the SA for an egress packet.


5.    (Original) The method of claim 1 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.


6.    (Original) The method of claim 1 wherein the lookup table entry comprises the key value and the index.

7.      (Original) The method of claim 6 wherein the lookup table entry further comprises a counter to track collisions for the entry.

8.      (Previously Presented) The method of claim 1 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

9.      (Canceled)

10.     (Original) The method of claim 1 further comprising supporting a number of network traffic streams, wherein the lookup table has $2^N$ entries, where N is an integer, $2^N$ being the lowest binary number greater than five times the number of network traffic streams supported.

11.     (Previously Presented) The method of claim 1 wherein hashing the key value comprises using a bit-wise AND hash function with a mask of value $2^N$-1, where N is an integer, wherein the hash table contains $2^N$ entries.

12.     (Previously Presented) An article comprising a machine-accessible medium to provide content to cause one or more electronic systems to:
        receive at a device driver a network packet having a corresponding security association (SA);
        determine if the packet is an ingress packet or an egress packet;
        determine for the packet a key value corresponding to the SA;
        if the packet is an ingress packet, hash the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hash the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;
        retrieve from the entry an index to a location of the SA in memory; and
        retrieve the SA from memory based on the index.

**13.** (Previously Presented) The article of claim 12 wherein to receive the network packet comprises the device driver to be passed an egress packet from an electronic system operating system.

**14.** (Previously Presented) The article of claim 12 wherein to receive the network packet comprises the device driver to be passed an ingress packet from a network interface device.

**15.** (Original) The article of claim 12 wherein the key value is a handle created for the SA for an egress packet.

**16.** (Original) The article of claim 12 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

**17.** (Original) The article of claim 12 wherein the lookup table entry comprises the key value and the index.

**18.** (Original) The article of claim 17 wherein the lookup table entry further comprises a counter to track collisions for the entry.

**19.** (Previously Presented) The article of claim 12 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

**20.** (Canceled)

**21.** (Original) The article of claim 12 further comprising to support a number of network traffic streams, wherein the lookup table has $2^N$ entries, where N is an integer, $2^N$ being the lowest binary number greater than five times the number of network traffic streams supported.

**22.** (Previously Presented) The article of claim 12 wherein to hash the key value comprises using a bit-wise AND hash function with a mask of value $2^N-1$, where N is an integer, wherein the hash table contains $2^N$ entries.

**23.** (Previously Presented) An electronic data signal embodied in a data communications medium shared among a plurality of network devices comprising content to cause one or more electronic systems to:

receive at a device driver a network packet having a corresponding security association (SA);

determine if the packet is an ingress packet or an egress packet;

determine for the packet a key value corresponding to the SA;

if the packet is an ingress packet, hash the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hash the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;

retrieve from the entry an index to a location of the SA in memory; and

retrieve the SA from memory based on the index.

**24.** (Previously Presented) The electronic data signal of claim 23 wherein to receive the network packet comprises the device driver to be passed an egress packet from an electronic system operating system.

**25.** (Previously Presented) The electronic data signal of claim 23 wherein to receive the network packet comprises the device driver to be passed an ingress packet from a network interface device.

**26.** (Original) The electronic data signal of claim 23 wherein the key value is a handle created for the SA for an egress packet.

**27.** (Original) The electronic data signal of claim 23 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

**28.** (Original) The electronic data signal of claim 23 wherein the lookup table entry comprises the key value and the index.

**29.** (Original) The electronic data signal of claim 28 wherein the lookup table entry further comprises a counter to track collisions for the entry.

**30.** (Previously Presented) The electronic data signal of claim 23 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

**31.** (Canceled)

**32.** (Original) The electronic data signal of claim 23 further comprising to support a number of network traffic streams, wherein the lookup table has $2^N$ entries, where N is an integer, $2^N$ being the lowest binary number greater than five times the number of network traffic streams supported.

**33.** (Previously Presented) The electronic data signal of claim 23 wherein to hash the key value comprises using a bit-wise AND hash function with a mask of value $2^N-1$, where N is an integer, wherein the hash table contains $2^N$ entries.

**34.** (Previously Presented) An electronic system comprising:

one or more processors;

a network interface coupled with the one or more processors to provide a communications path between the electronic system and a network, the network interface to have a corresponding device driver to be executed on one or more of the processors; and

a memory coupled with the one or more processors, the memory to have a program to provide instructions for the electronic system to receive at the device driver a network packet having a corresponding security association (SA), the program to determine if the packet is an ingress packet or an egress packet, to determine for the packet a key value corresponding to the SA, and if the packet is an ingress packet, hash the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hash the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table, to retrieve from the entry an index to a location of the SA in memory, and to retrieve the SA from memory based on the index.

35.    (Previously Presented) The electronic system of claim 34 wherein the program to receive the network packet comprises the device driver to be passed an egress packet from an operating system.

36.    (Previously Presented) The electronic system of claim 34 wherein the program to receive the network packet comprises the device driver to be passed an ingress packet from the network interface.

37.    (Original) The electronic system of claim 34 wherein the key value is a handle created for the SA for an egress packet.

38.    (Original) The electronic system of claim 34 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

39.    (Original) The electronic system of claim 34 wherein the lookup table entry comprises the key value and the index.

40.    (Original) The electronic system of claim 39 wherein the lookup table entry further comprises a counter to track collisions for the entry.

**41.** (Previously Presented) The electronic system of claim 34 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

**42.** (Canceled)

**43.** (Original) The electronic system of claim 34 further comprising the program to support a number of network traffic streams, wherein the lookup table has $2^N$ entries, where N is an integer, $2^N$ being the lowest binary number greater than five times the number of network traffic streams supported.

**44.** (Previously Presented) The electronic system of claim 34 wherein to hash the key value comprises using a bit-wise AND hash function with a mask of value $2^N-1$, where N is an integer, wherein the hash table contains $2^N$ entries.